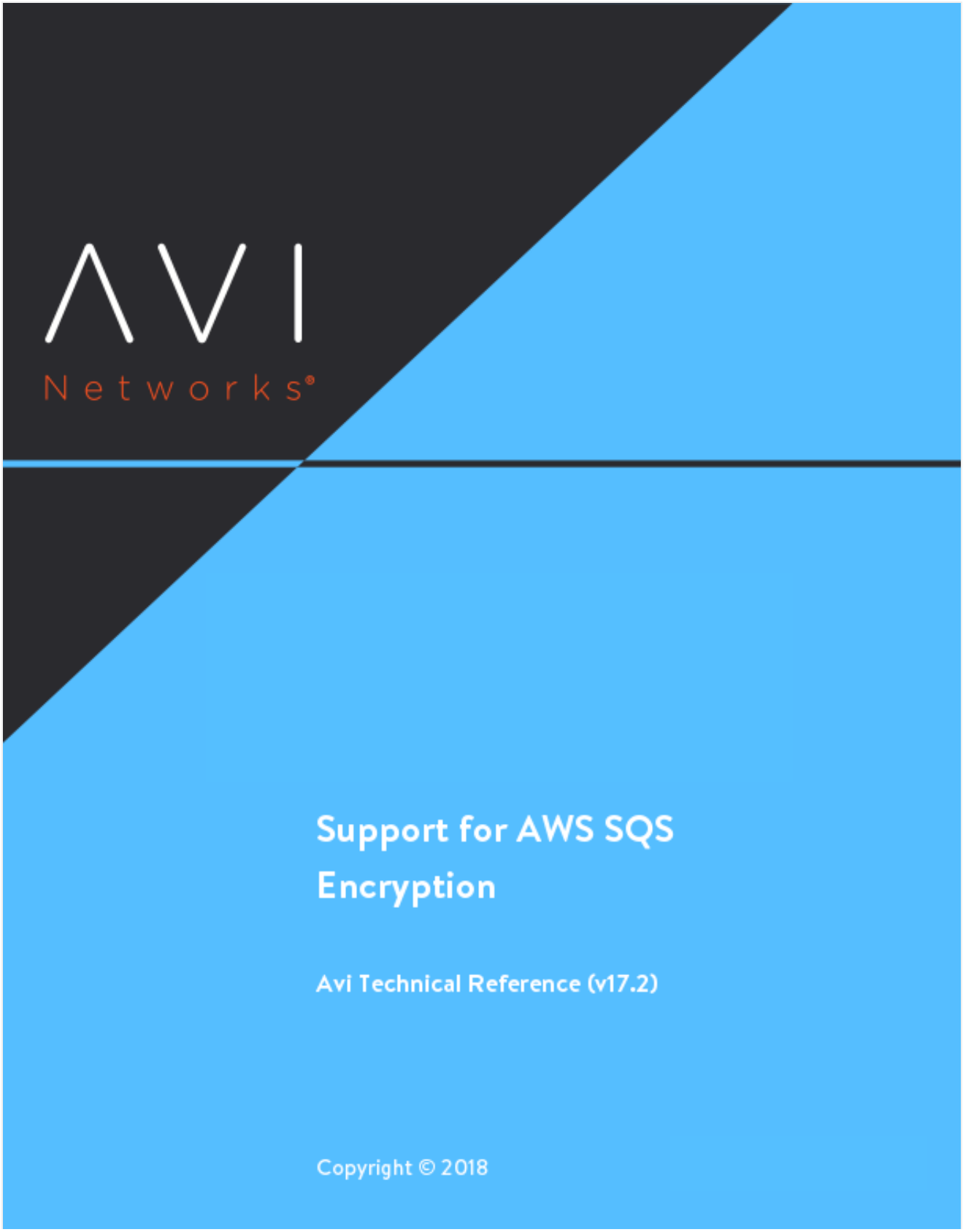


Support for AWS SQS Encryption

Avi Technical Reference (v17.2)

Support for AWS SQS Encryption

view online

Server-Side Encryption (SSE) of Amazon Simple Queue Service (SQS) message queues is supported by Avi Vantage starting in release 17.2.8. Encrypting a queue does *not* encrypt backlogged messages, *nor* does turning off encryption remove encryption from backlogged messages. SQS queue encryption is supported only in 3 AWS regions as of the time of this writing: US EAST (N. Virginia), US EAST (Ohio), and US WEST (Oregon).

Prerequisites

For the Avi Controller to work with encrypted SQS queues and other artifacts of Amazon Simple Notification Service (SNS), either the user whose access/secret key is used or the `AviController-Refined-Role` must have the following policies attached to it:

- `AviController-SQS-Policy`
- `AviController-SNS-Policy`
- `AviController-KMS-Policy`

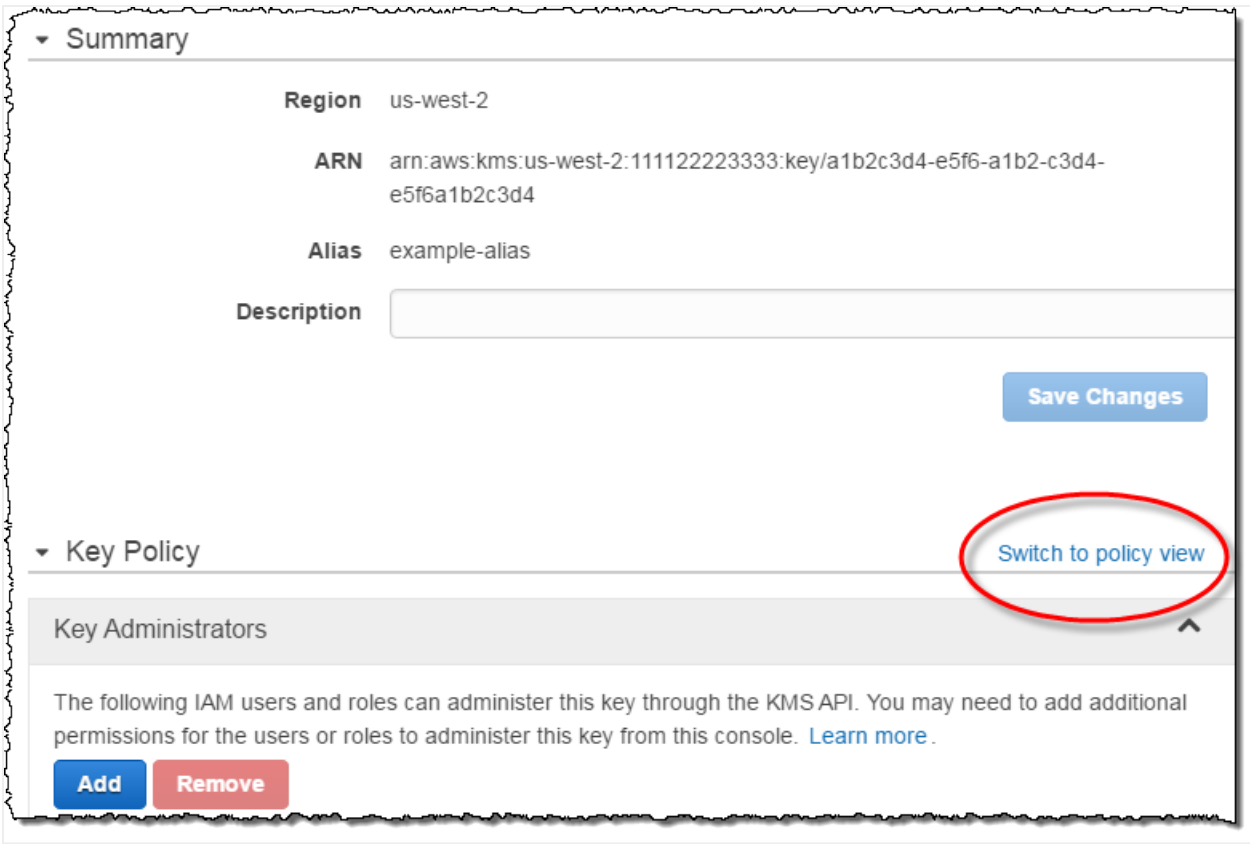
The `AviController-Refined-Role` must be able to decrypt received messages when polling SQS queues. For this, the `AviController-KMS-Policy` must be updated to include within it a write action, `kms:Decrypt`. JSON files for this role and policy are shown in the IAM Role Setup for Installation article.

Customer Managed Customer Master Keys

The primary resources in the AWS Key Management Service are customer master keys (CMKs). Customer managed CMKs are CMKs the user creates, manages, and uses (contrast them with AWS managed CMKs, which are created, managed, and used on the user's behalf by an AWS service that is integrated with AWS KMS). This includes enabling and disabling the CMK, rotating its cryptographic material, and establishing the IAM policies and key policies that govern access to the CMK, as well as using the CMK in cryptographic operations. SSE of an SQS queue is done using a customer managed CMK, and an SNS topic must be able to make use of that encryption key to encrypt/decrypt a message that it wants to send to the queue. For this, the encryption key's policy must be modified to allow SNS service to work with it.

Adding Necessary Permissions to Customer Managed CMKs

1. Sign in to the AWS Management Console and open the AWS Identity and Access Management (IAM) console.
2. In the left navigation pane, choose Encryption keys.
3. For Region, choose the appropriate AWS Region.
4. Choose the alias of the CMK whose key policy document you want to edit.
5. On the Key Policy line, choose Switch to policy view.



1. Add following statement in the key policy.

```
{
     "Sid": "Allow SNS to use CMK",
     "Effect": "Allow",
     "Principal": {
       "Service": "sns.amazonaws.com"
     },
     "Action": [
       "kms:GenerateDataKey*",
       "kms:Decrypt"
     ],
     "Resource": "*"
    }
```

Configuration Steps to Enable SQS Queue Encryption through Avi UI

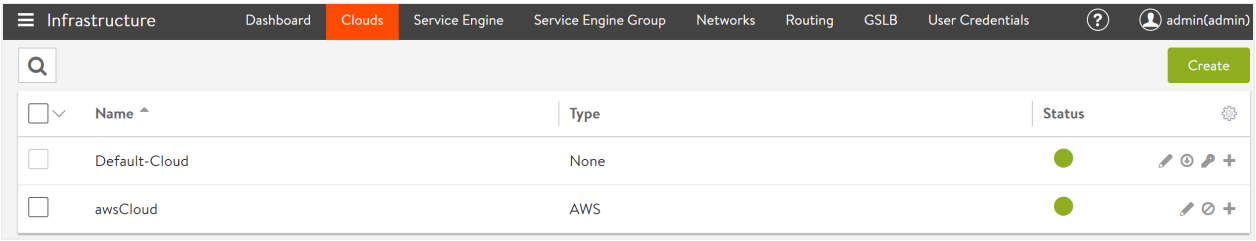
Starting with Avi Vantage 17.2.10, SQS queue encryption option for an AWS cloud can be enabled through the Avi UI as well.

Note: Enabling SQS queue encryption through the Avi UI is available only for the following AWS regions: * US East (N. Virginia) * US East (Ohio) * US West (Oregon)

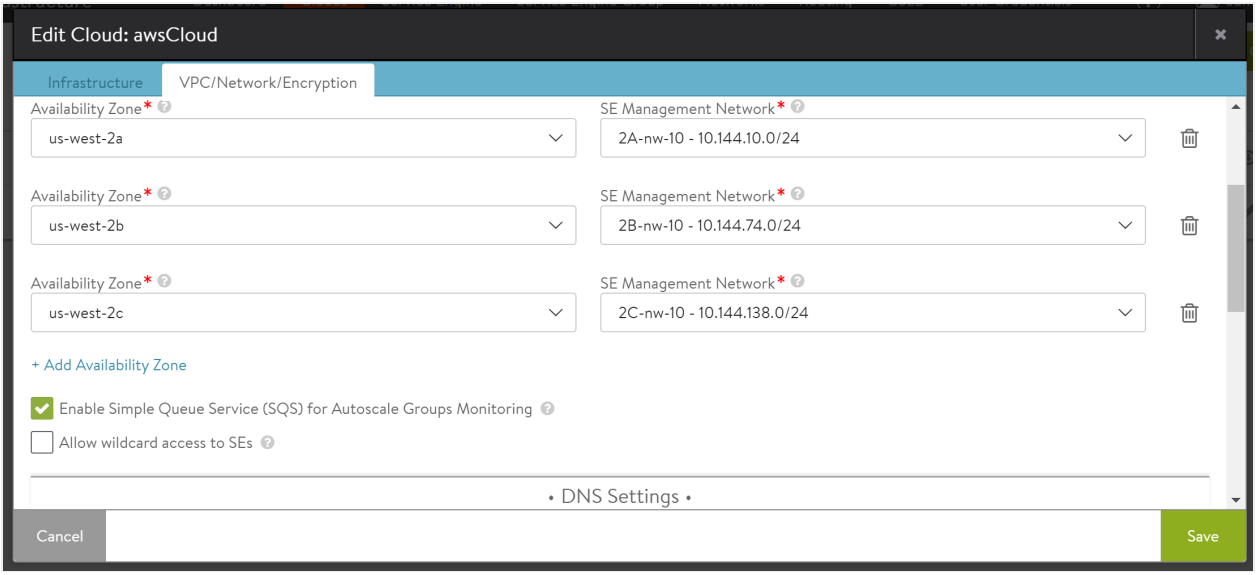
During the cloud creation steps, select one of the AWS regions mentioned above.

Follow the steps mentioned below to enable SQS queue encryption through the Avi UI:

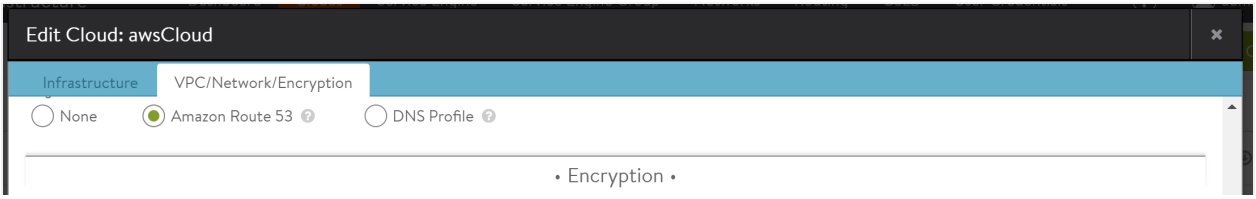
- Navigate to Infrastructure > Clouds, click on Create to create a new cloud or use the edit icon to edit the existing cloud.

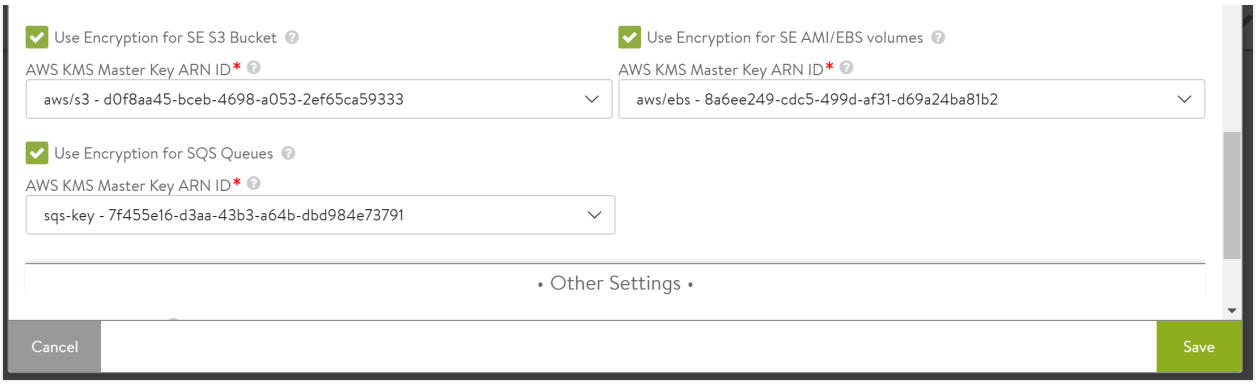


- Select VPC/Network/Encryption option, and enable the checkbox for Enable Simple Queue Service (SQS) for Autoscale Groups Monitoring available under the AWS VPC and Availability Zones section.



- Select Use Encryption for SQS Queue available under the Encryption section, and select value for AWS KMS Master Key ARN ID from the drop-down menu as shown below.





- Click on Save to save the changes.

Avi Vantage CLI Commands to Enable SQS Queue Encryption

Substituting your cloud name and key_id as appropriate, type these CLI commands into the Avi `shell`:

```
[admin:10-144-6-46]: > configure cloud cloudAWS
[admin:10-144-6-46]: cloud> aws_configuration
[admin:10-144-6-46]: cloud:aws_configuration> sqs_encryption
[admin:10-144-6-46]: cloud:aws_configuration:sqs_encryption> mode aws_encryption_mode_sse_kms
[admin:10-144-6-46]: cloud:aws_configuration:sqs_encryption> master_key <key_id>
[admin:10-144-6-46]: cloud:aws_configuration:sqs_encryption> save
```